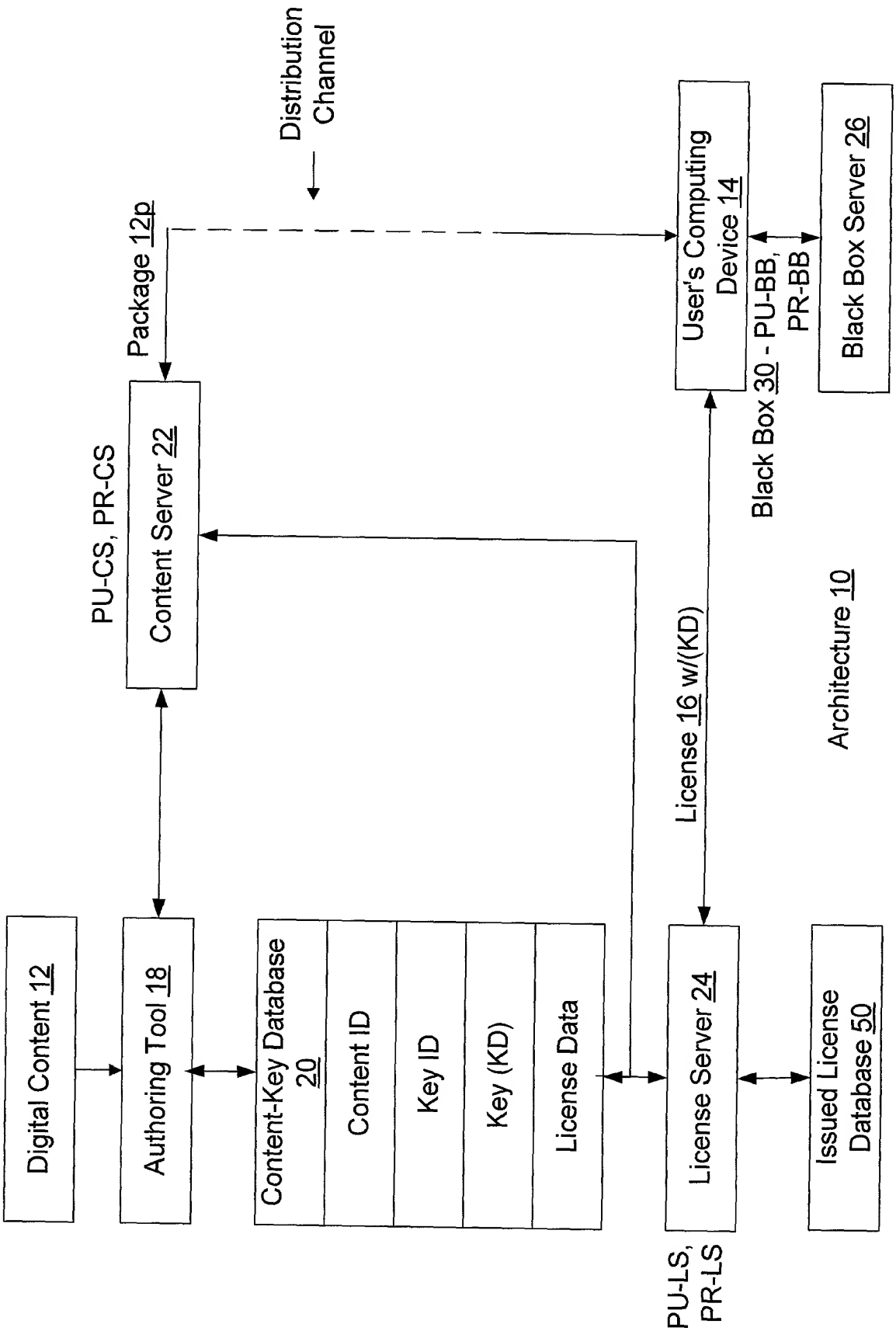
Distribution Channel
Package 12p
User's Computing Device 14
Black Box Server 26
Black Box 30 - PU-BB, PR-BB
PU-CS, PR-CS
Content Server 22
License 16 w/(KD)
Digital Content 12
Authoring Tool 18
Content-Key Database 20
Content ID
Key ID
Key (KD)
License Data
License Server 24
Issued License Database 50
PU-LS, PR-LS
Architecture 10

Fig. 1

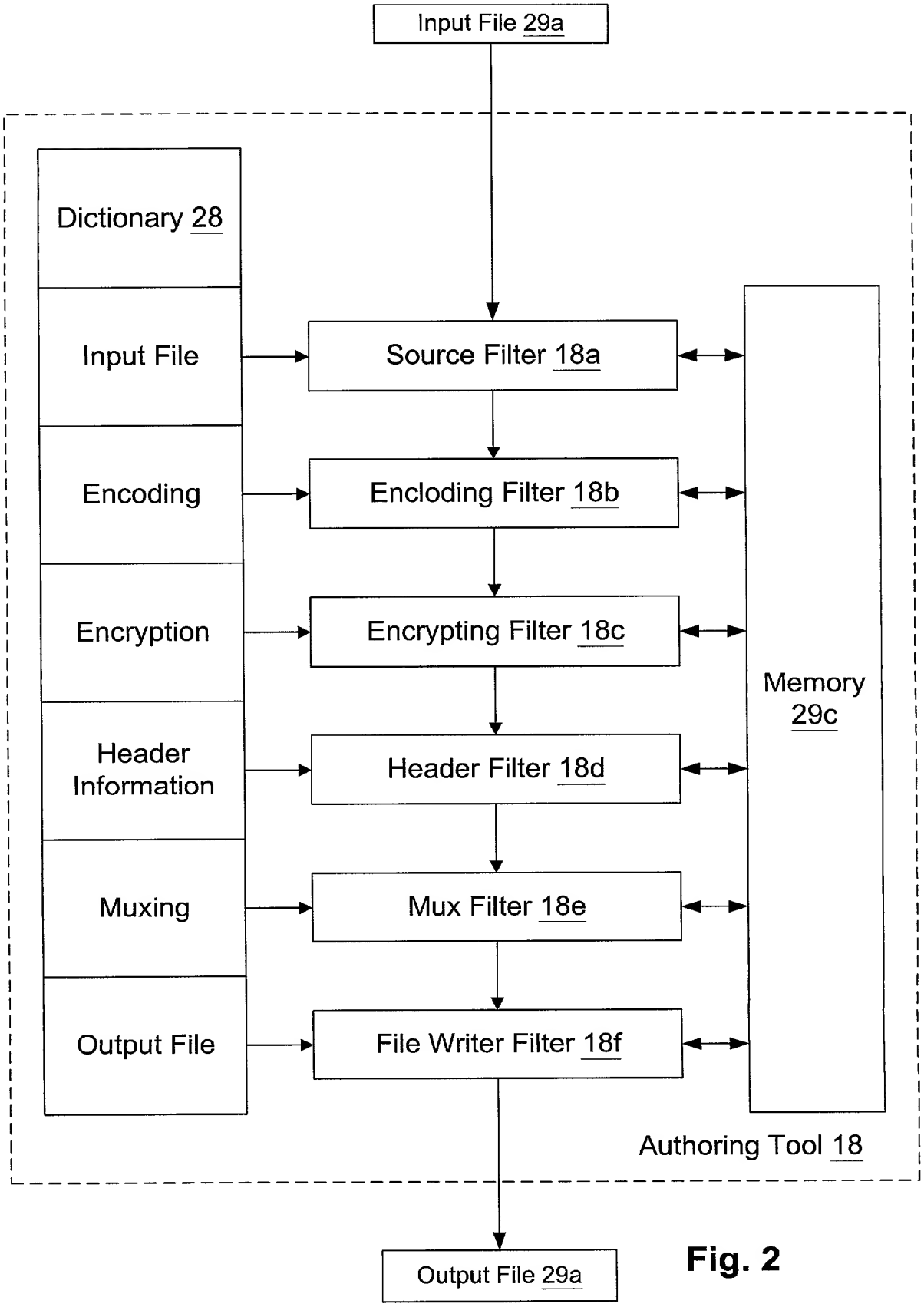
Input File 29a
Dictionary 28
Input File
Encoding
Encryption
Header Information
Muxing
Output File
Source Filter 18a
Encloding Filter 18b
Encrypting Filter 18c
Header Filter 18d
Mux Filter 18e
File Writer Filter 18f
Memory 29c
Authoring Tool 18
Output File 29a

Fig. 2

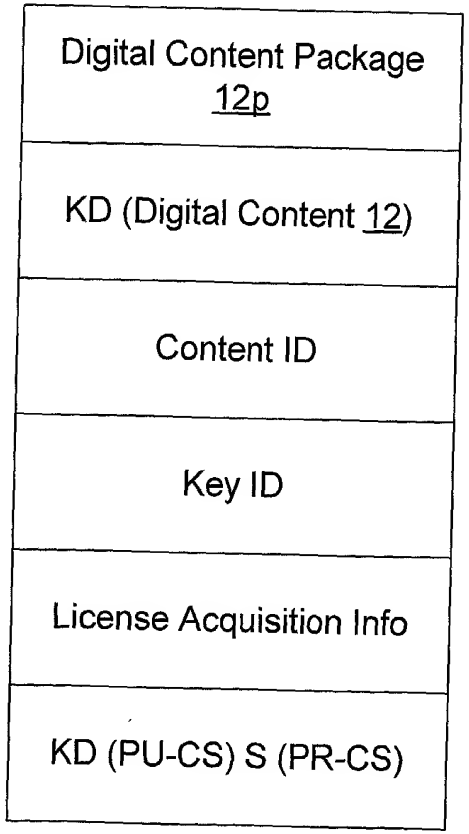
Digital Content Package 12p
KD (Digital Content 12)
Content ID
Key ID
License Acquisition Info
KD (PU-CS) S (PR-CS)

Fig. 3

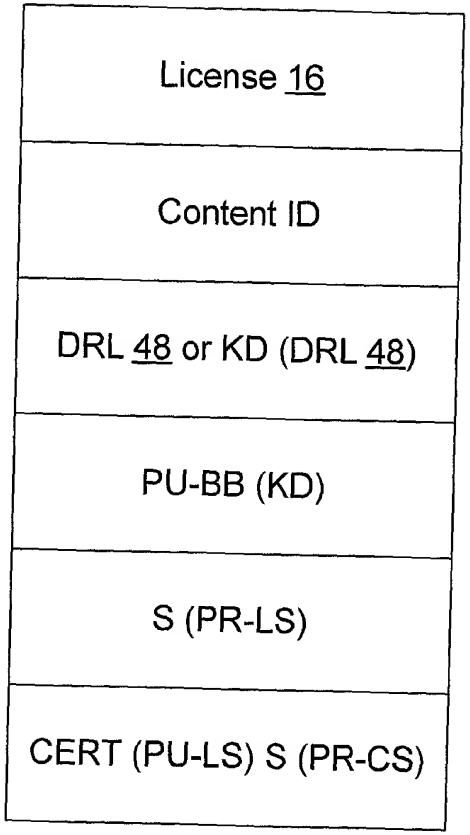
License 16
Content ID
DRL 48 or KD (DRL 48)
PU-BB (KD)
S (PR-LS)
CERT (PU-LS) S (PR-CS)

Fig. 8

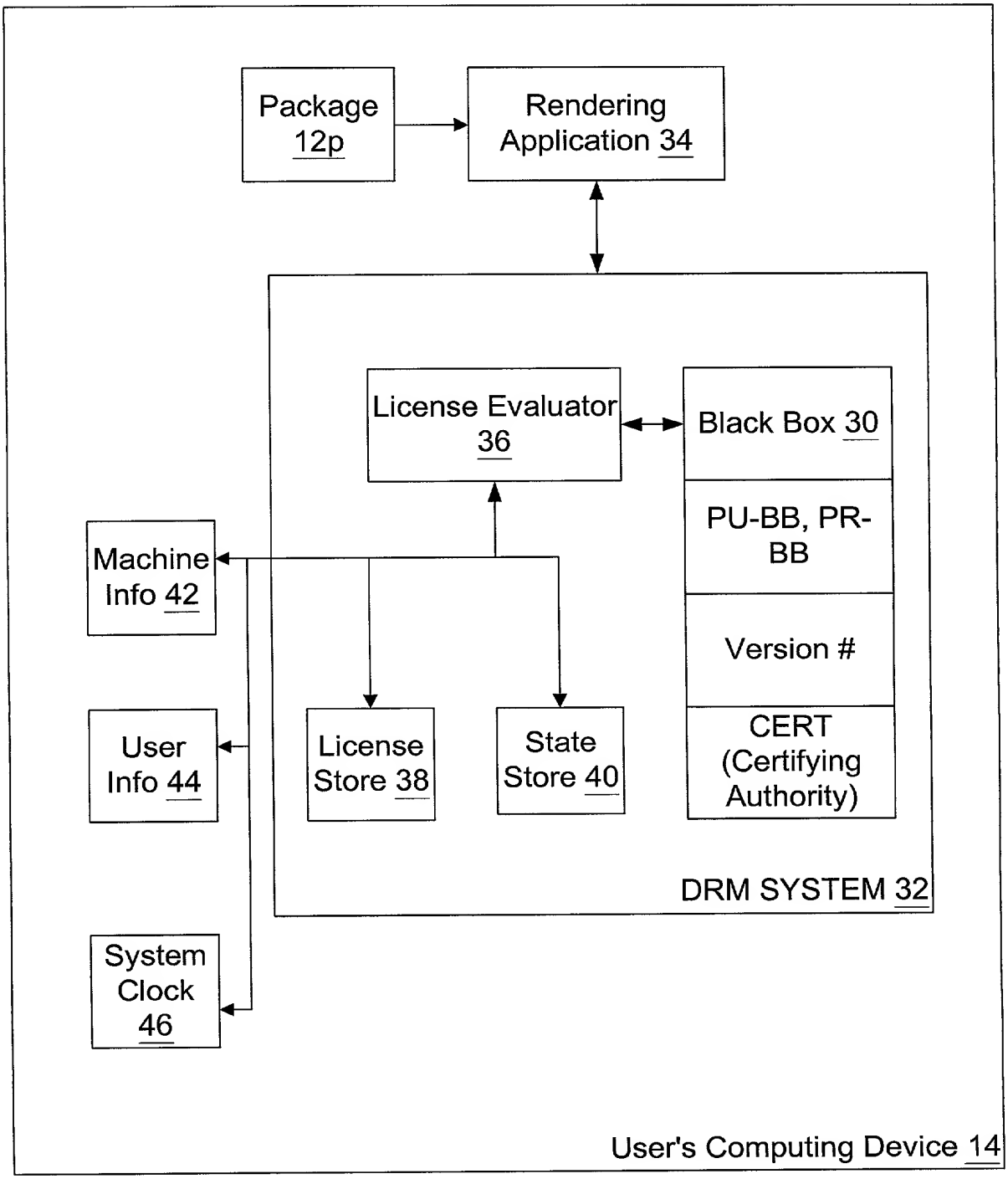
Package 12p
Rendering Application 34
License Evaluator 36
Black Box 30
PU-BB, PR-BB
Version #
CERT (Certifying Authority)
Machine Info 42
User Info 44
License Store 38
State Store 40
DRM SYSTEM 32
System Clock 46
User's Computing Device 14

Fig. 4

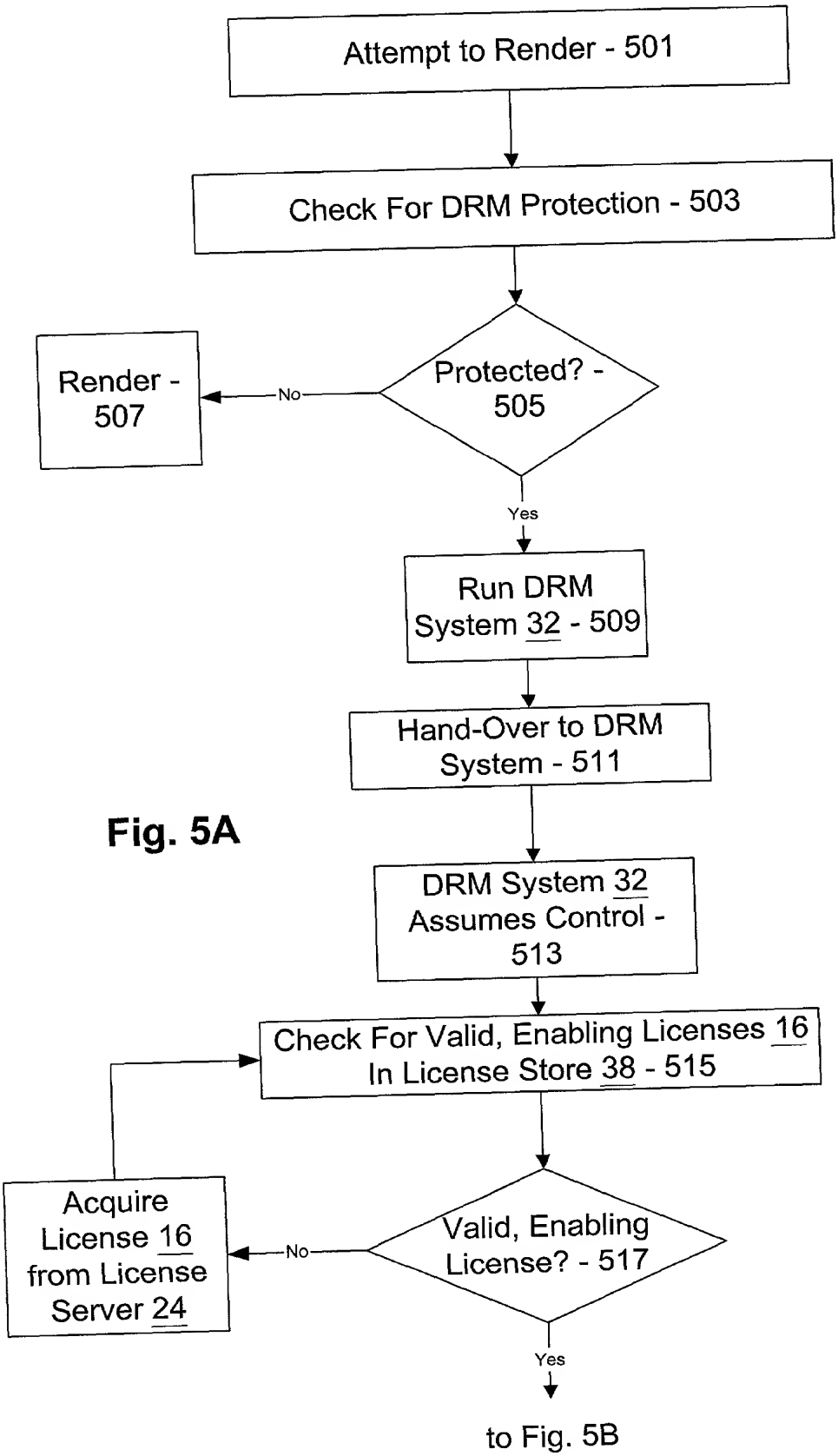
Attempt to Render - 501
Check For DRM Protection - 503
Protected? - 505
No
Render - 507
Yes
Run DRM System 32 - 509
Hand-Over to DRM System - 511
DRM System 32 Assumes Control - 513
Check For Valid, Enabling Licenses 16 In License Store 38 - 515
Valid, Enabling License? - 517
No
Acquire License 16 from License Server 24
Yes
to Fig. 5B

Fig. 5A

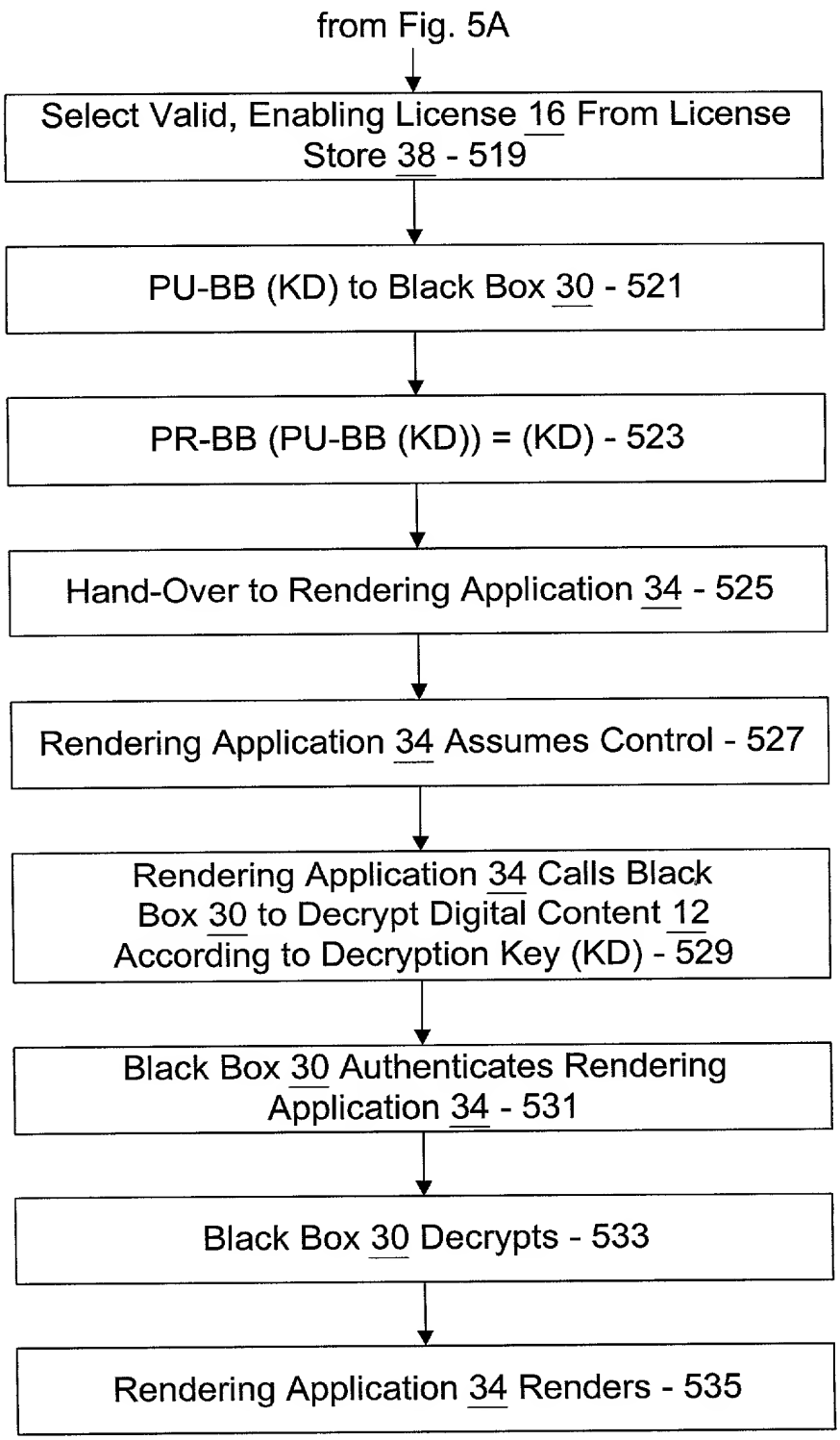
from Fig. 5A
Select Valid, Enabling License 16 From License Store 38 - 519
PU-BB (KD) to Black Box 30 - 521
PR-BB (PU-BB (KD)) = (KD) - 523
Hand-Over to Rendering Application 34 - 525
Rendering Application 34 Assumes Control - 527
Rendering Application 34 Calls Black Box 30 to Decrypt Digital Content 12 According to Decryption Key (KD) - 529
Black Box 30 Authenticates Rendering Application 34 - 531
Black Box 30 Decrypts - 533
Rendering Application 34 Renders - 535

Fig. 5B

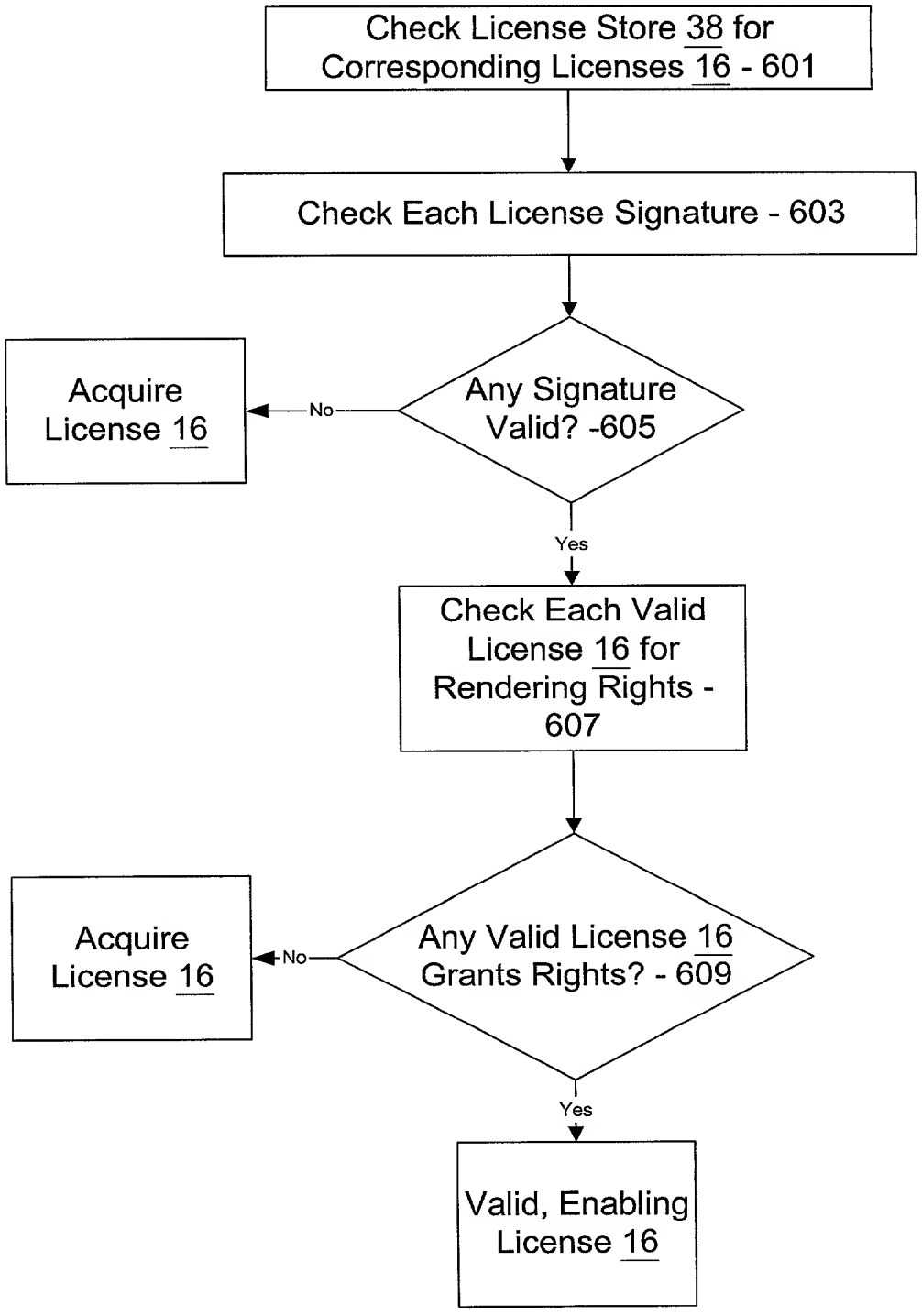
Check License Store 38 for Corresponding Licenses 16 - 601
Check Each License Signature - 603
Any Signature Valid? -605
No
Acquire License 16
Yes
Check Each Valid License 16 for Rendering Rights - 607
Any Valid License 16 Grants Rights? - 609
No
Acquire License 16
Yes
Valid, Enabling License 16

Fig. 6

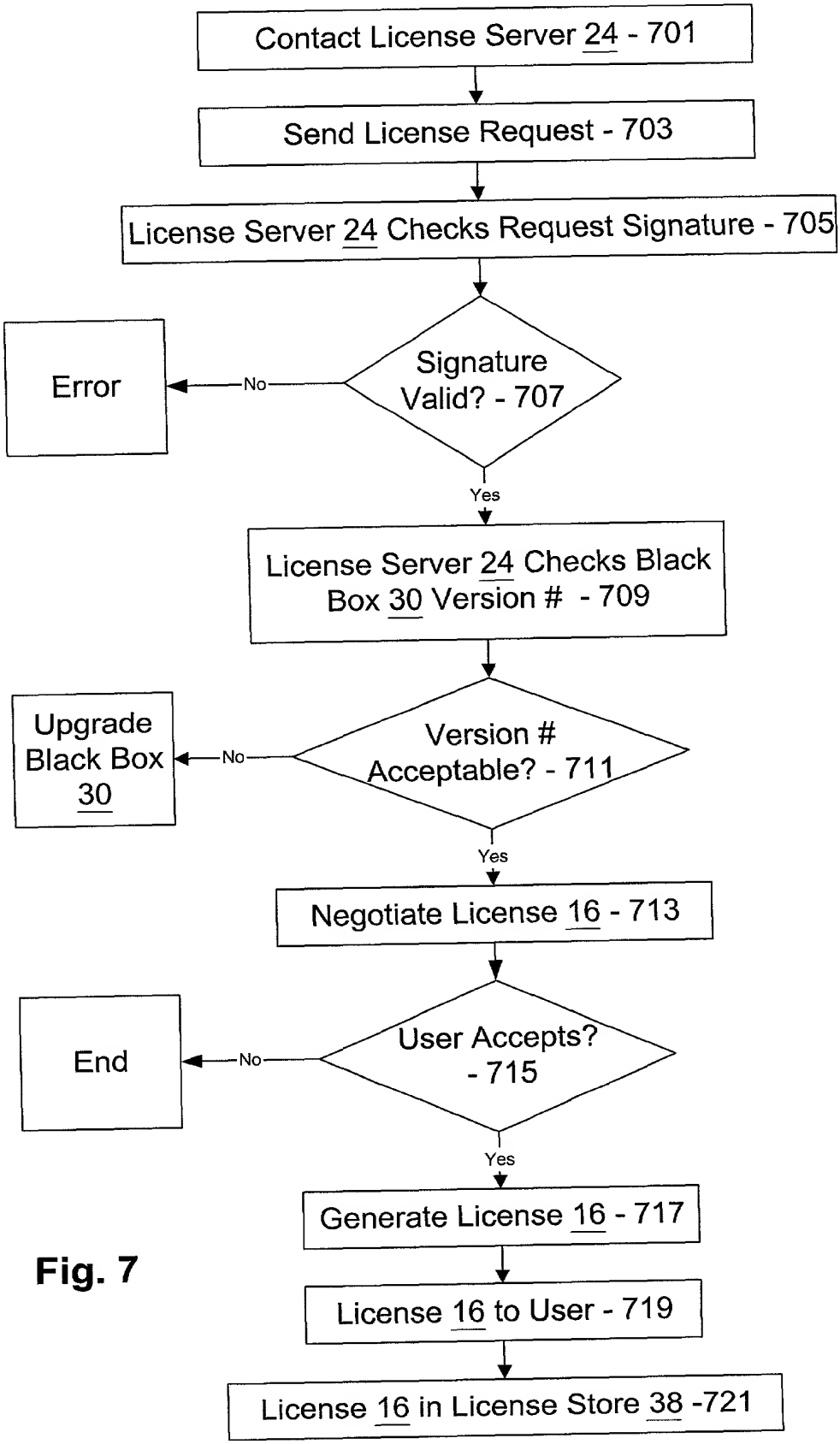
Contact License Server 24 - 701
Send License Request - 703
License Server 24 Checks Request Signature - 705
Signature Valid? - 707
No
Error
Yes
License Server 24 Checks Black Box 30 Version # - 709
Version # Acceptable? - 711
No
Upgrade Black Box 30
Yes
Negotiate License 16 - 713
User Accepts? - 715
No
End
Yes
Generate License 16 - 717
License 16 to User - 719
License 16 in License Store 38 -721

Fig. 7

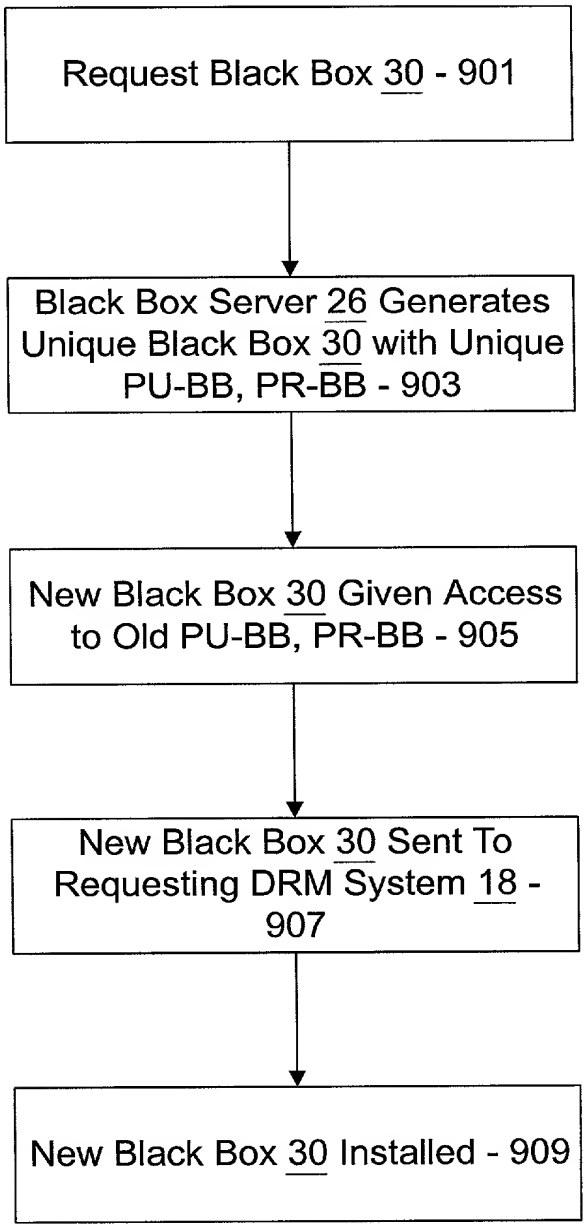
Request Black Box 30 - 901
Black Box Server 26 Generates Unique Black Box 30 with Unique PU-BB, PR-BB - 903
New Black Box 30 Given Access to Old PU-BB, PR-BB - 905
New Black Box 30 Sent To Requesting DRM System 18 - 907
New Black Box 30 Installed - 909

Fig. 9

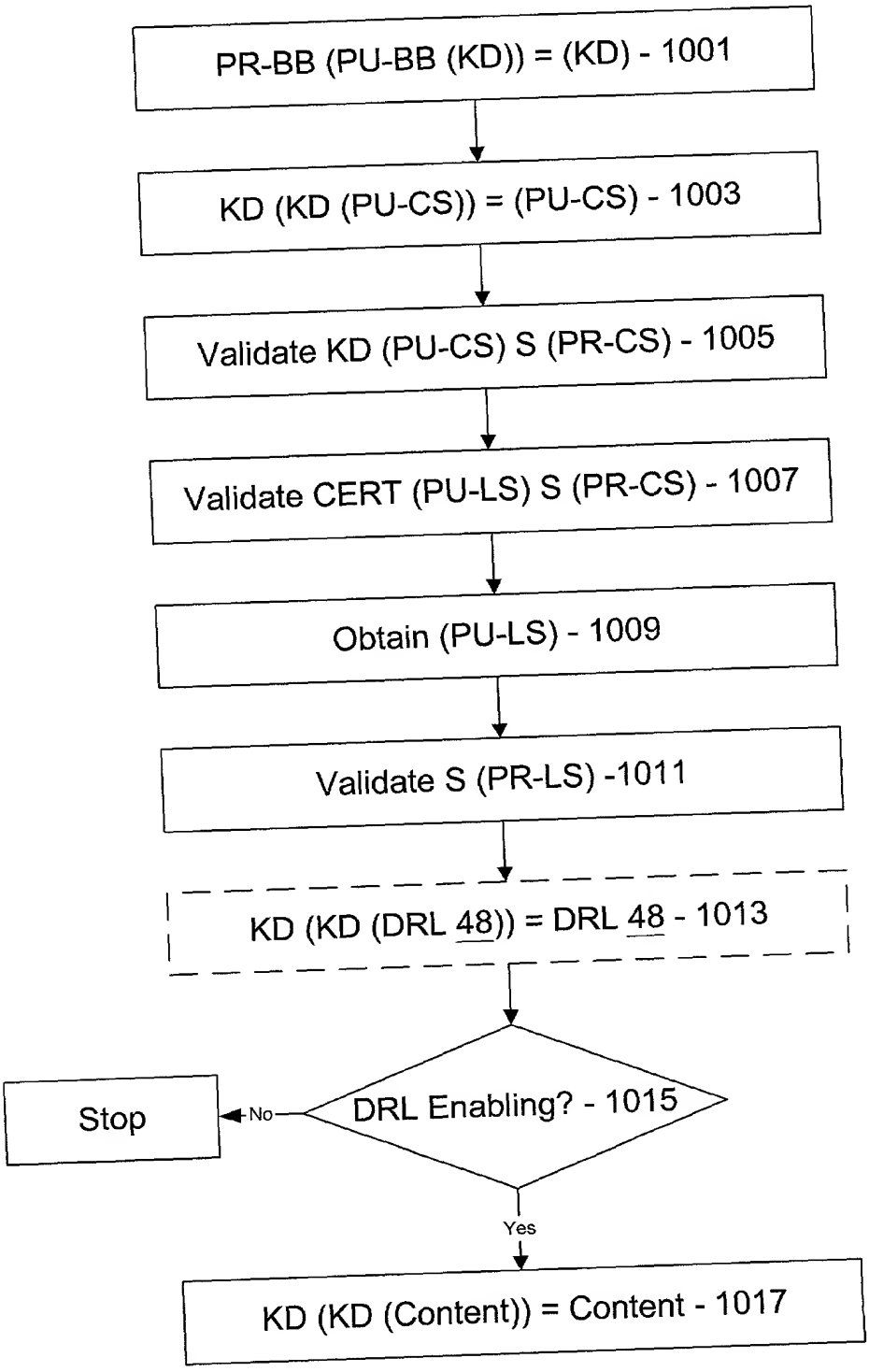
PR-BB (PU-BB (KD)) = (KD) - 1001
KD (KD (PU-CS)) = (PU-CS) - 1003
Validate KD (PU-CS) S (PR-CS) - 1005
Validate CERT (PU-LS) S (PR-CS) - 1007
Obtain (PU-LS) - 1009
Validate S (PR-LS) -1011
KD (KD (DRL 48)) = DRL 48 - 1013
DRL Enabling? - 1015
No
Stop
Yes
KD (KD (Content)) = Content - 1017

Fig. 10

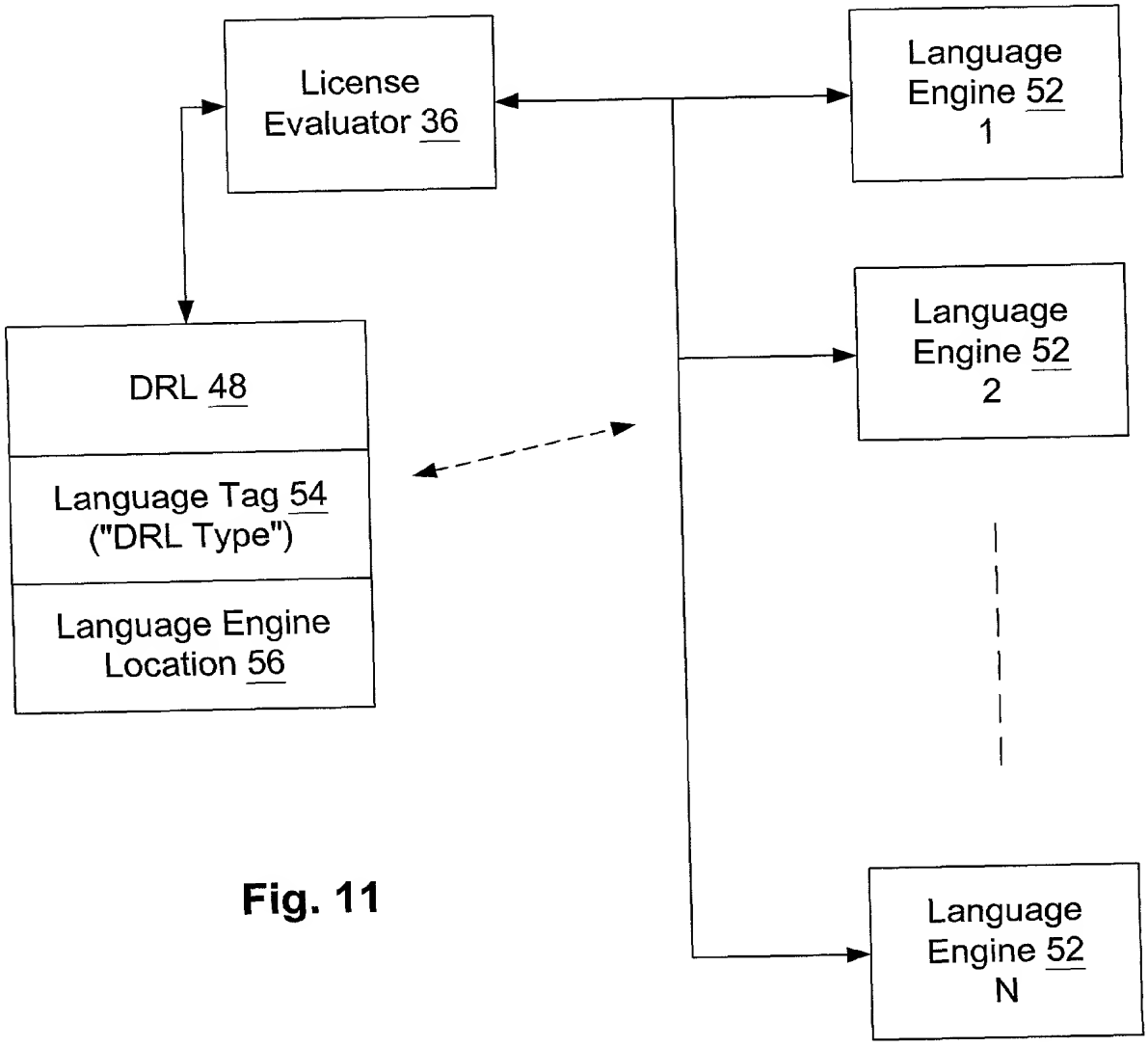
License Evaluator 36
Language Engine 52 1
Language Engine 52 2
Language Engine 52 N
DRL 48
Language Tag 54 ("DRL Type")
Language Engine Location 56

Fig. 11

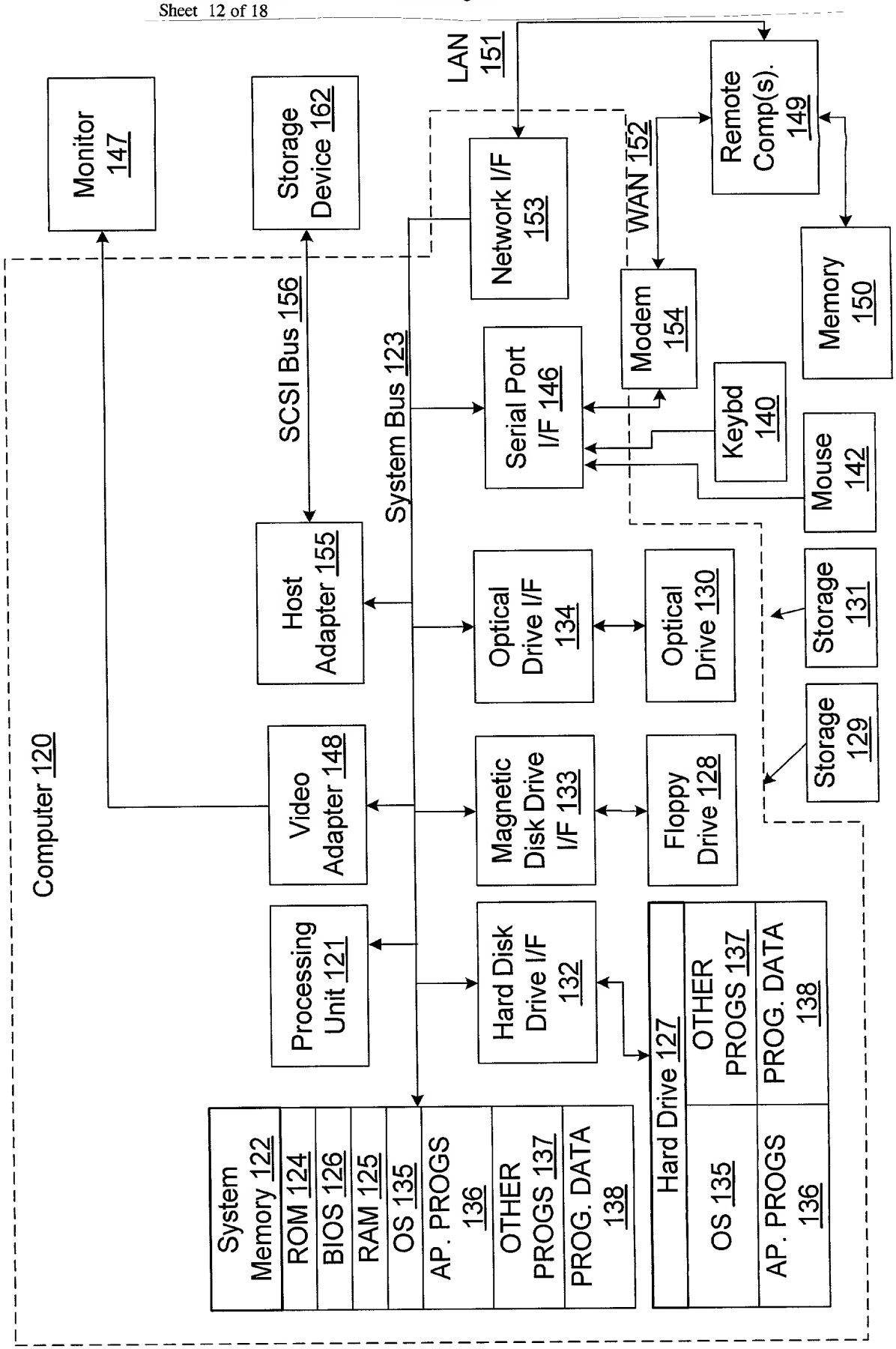
Computer 120
Monitor 147
Storage Device 162
LAN 151
Remote Comp(s). 149
Network I/F 153
WAN 152
Memory 150
SCSI Bus 156
System Bus 123
Modem 154
Serial Port I/F 146
Keybd 140
Mouse 142
Host Adapter 155
Optical Drive I/F 134
Optical Drive 130
Storage 131
Video Adapter 148
Magnetic Disk Drive I/F 133
Floppy Drive 128
Storage 129
Processing Unit 121
Hard Disk Drive I/F 132
System Memory 122
ROM 124
BIOS 126
RAM 125
OS 135
AP. PROGS 136
OTHER PROGS 137
PROG. DATA 138
Hard Drive 127
OS 135
AP. PROGS 136
OTHER PROGS 137
PROG. DATA 138

Fig. 12

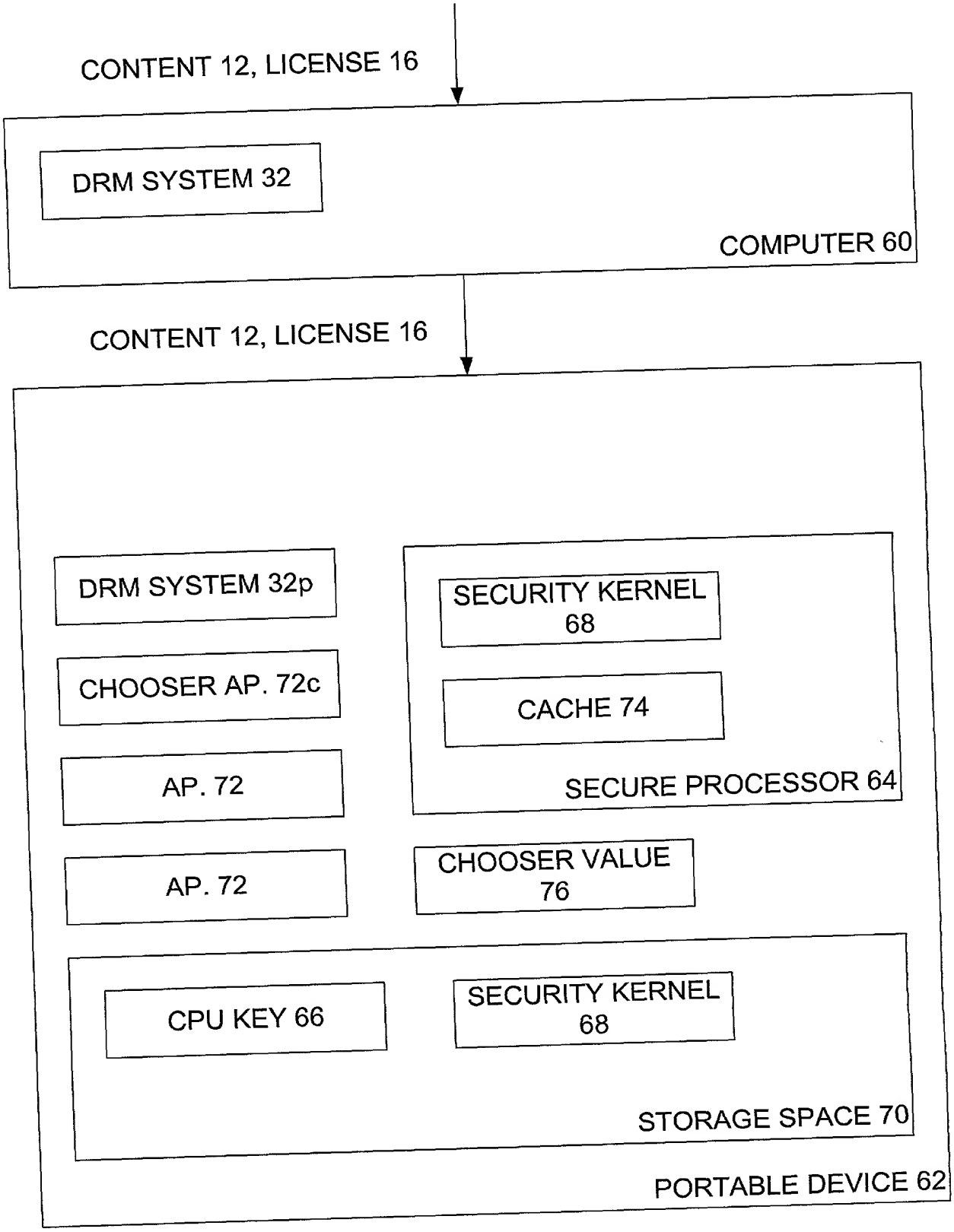
CONTENT 12, LICENSE 16
DRM SYSTEM 32
COMPUTER 60
CONTENT 12, LICENSE 16
DRM SYSTEM 32p
CHOOSER AP. 72c
AP. 72
AP. 72
SECURITY KERNEL 68
CACHE 74
SECURE PROCESSOR 64
CHOOSER VALUE 76
CPU KEY 66
SECURITY KERNEL 68
STORAGE SPACE 70
PORTABLE DEVICE 62

Fig. 13

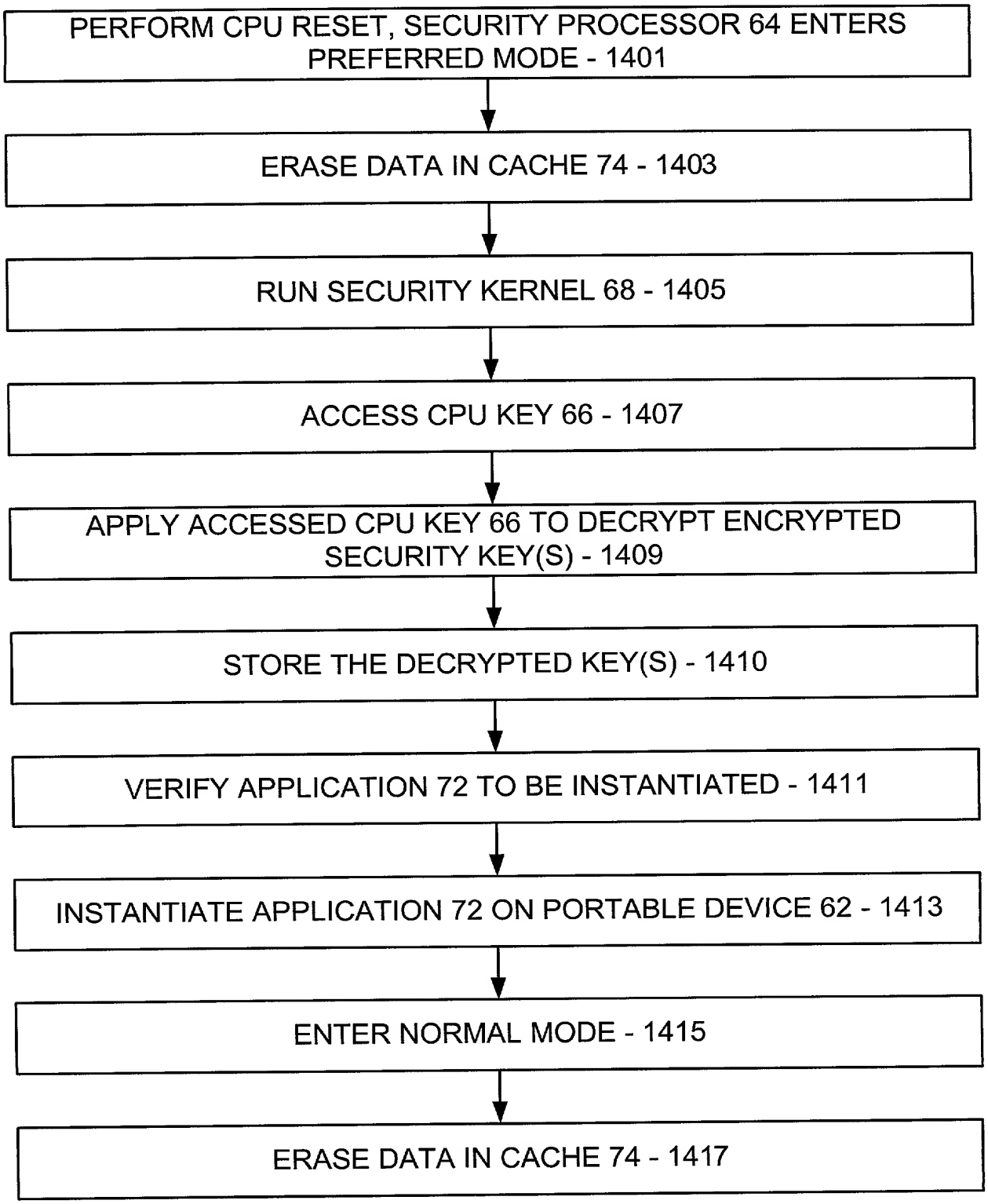
PERFORM CPU RESET, SECURITY PROCESSOR 64 ENTERS PREFERRED MODE - 1401
ERASE DATA IN CACHE 74 - 1403
RUN SECURITY KERNEL 68 - 1405
ACCESS CPU KEY 66 - 1407
APPLY ACCESSED CPU KEY 66 TO DECRYPT ENCRYPTED SECURITY KEY(S) - 1409
STORE THE DECRYPTED KEY(S) - 1410
VERIFY APPLICATION 72 TO BE INSTANTIATED - 1411
INSTANTIATE APPLICATION 72 ON PORTABLE DEVICE 62 - 1413
ENTER NORMAL MODE - 1415
ERASE DATA IN CACHE 74 - 1417

FIG. 14

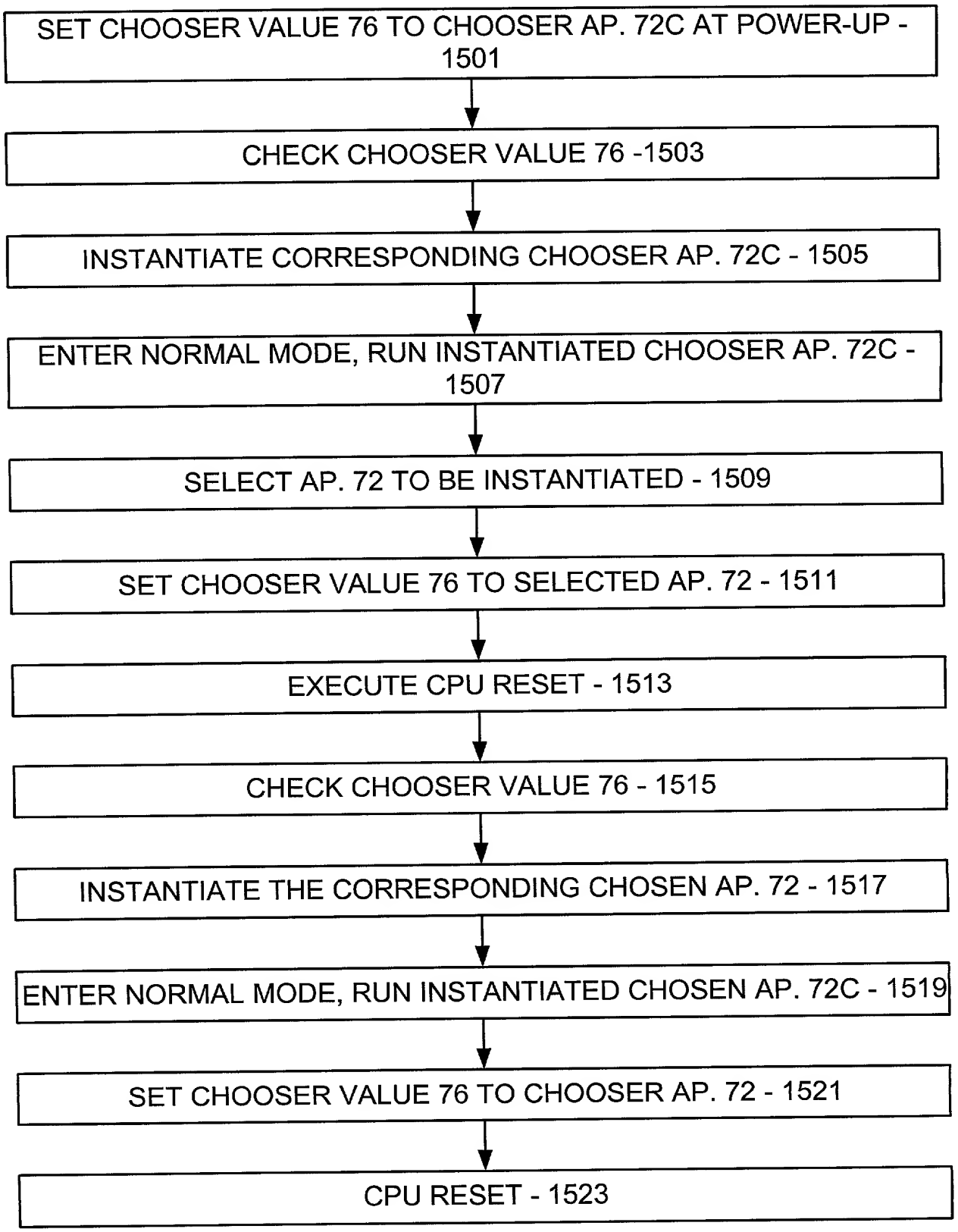
SET CHOOSER VALUE 76 TO CHOOSER AP. 72C AT POWER-UP - 1501
CHECK CHOOSER VALUE 76 -1503
INSTANTIATE CORRESPONDING CHOOSER AP. 72C - 1505
ENTER NORMAL MODE, RUN INSTANTIATED CHOOSER AP. 72C - 1507
SELECT AP. 72 TO BE INSTANTIATED - 1509
SET CHOOSER VALUE 76 TO SELECTED AP. 72 - 1511
EXECUTE CPU RESET - 1513
CHECK CHOOSER VALUE 76 - 1515
INSTANTIATE THE CORRESPONDING CHOSEN AP. 72 - 1517
ENTER NORMAL MODE, RUN INSTANTIATED CHOSEN AP. 72C - 1519
SET CHOOSER VALUE 76 TO CHOOSER AP. 72 - 1521
CPU RESET - 1523

FIG. 15

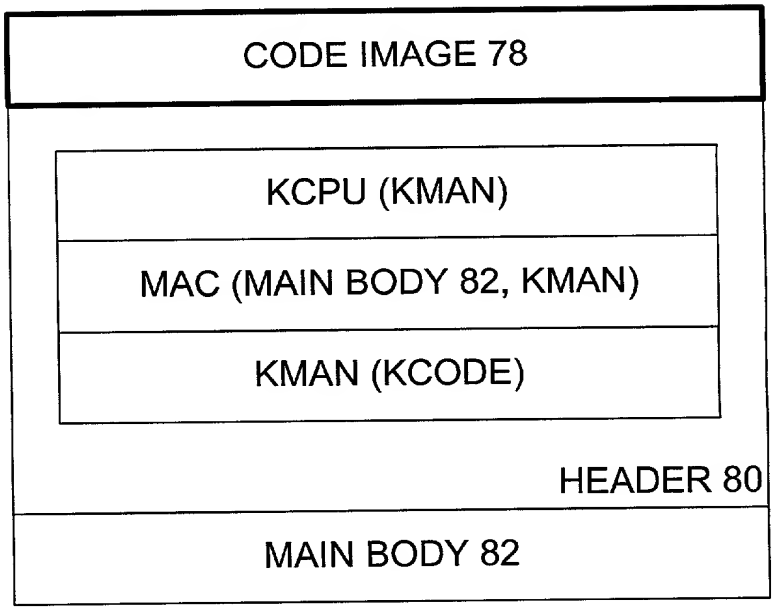
CODE IMAGE 78
KCPU (KMAN)
MAC (MAIN BODY 82, KMAN)
KMAN (KCODE)
HEADER 80
MAIN BODY 82

Fig. 16

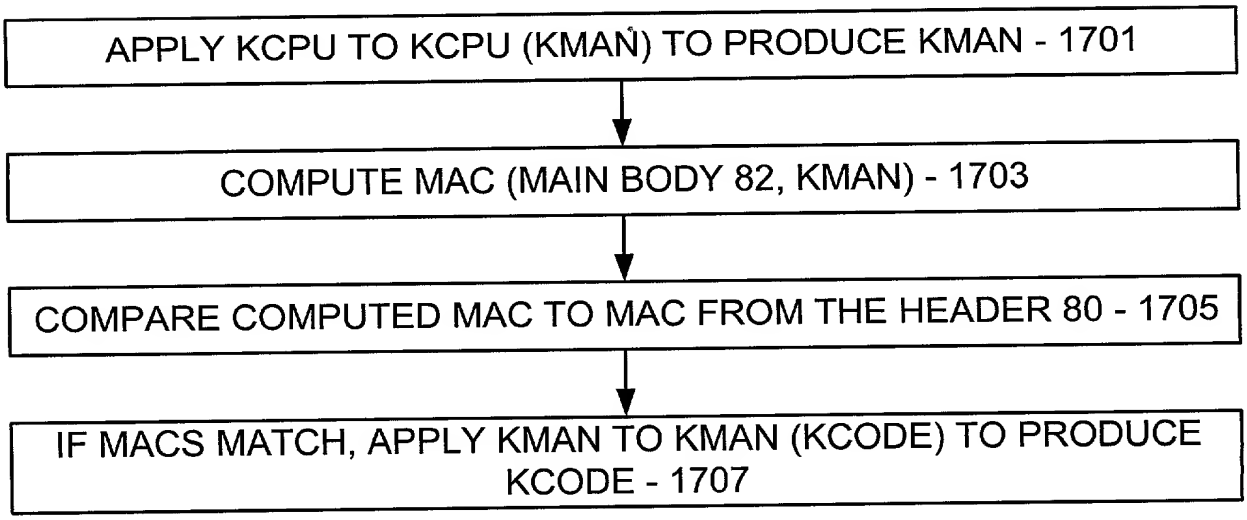
APPLY KCPU TO KCPU (KMAN) TO PRODUCE KMAN - 1701
COMPUTE MAC (MAIN BODY 82, KMAN) - 1703
COMPARE COMPUTED MAC TO MAC FROM THE HEADER 80 - 1705
IF MACS MATCH, APPLY KMAN TO KMAN (KCODE) TO PRODUCE KCODE - 1707

FIG. 17

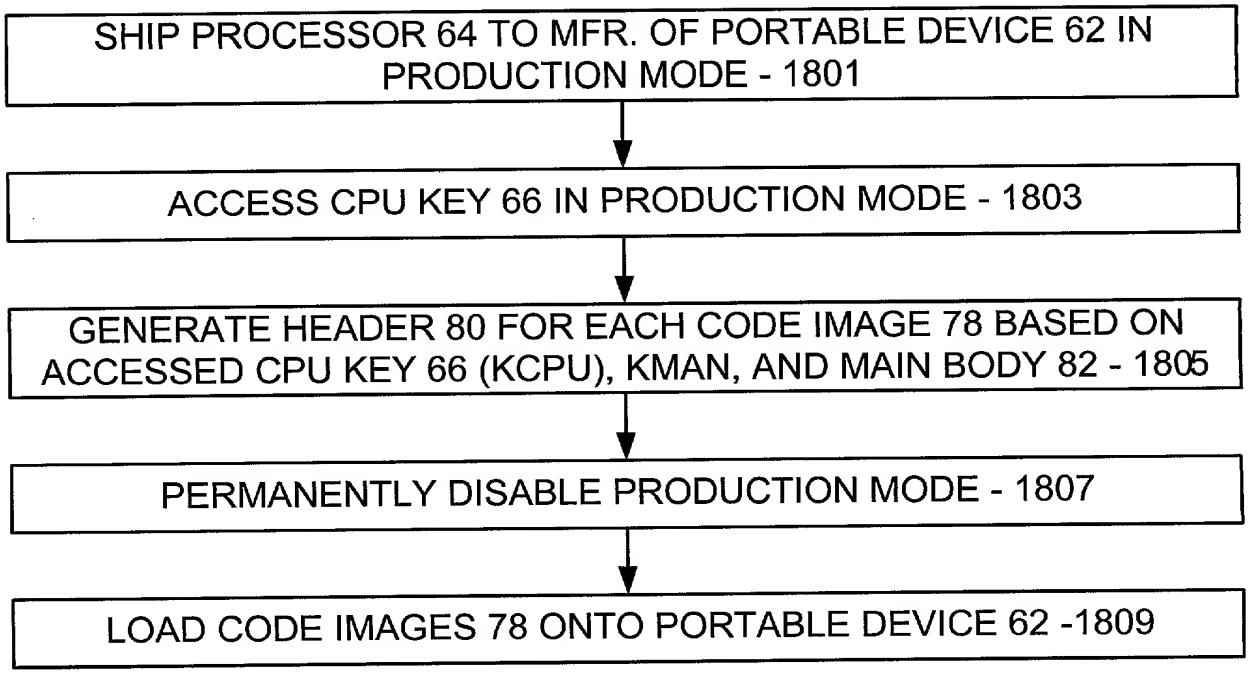
SHIP PROCESSOR 64 TO MFR. OF PORTABLE DEVICE 62 IN PRODUCTION MODE - 1801
ACCESS CPU KEY 66 IN PRODUCTION MODE - 1803
GENERATE HEADER 80 FOR EACH CODE IMAGE 78 BASED ON ACCESSED CPU KEY 66 (KCPU), KMAN, AND MAIN BODY 82 - 1805
PERMANENTLY DISABLE PRODUCTION MODE - 1807
LOAD CODE IMAGES 78 ONTO PORTABLE DEVICE 62 -1809

FIG. 18

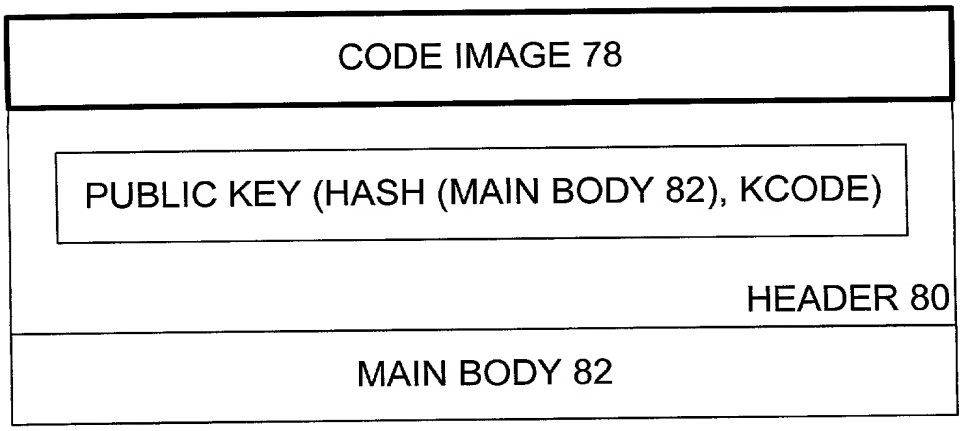

Fig. 19

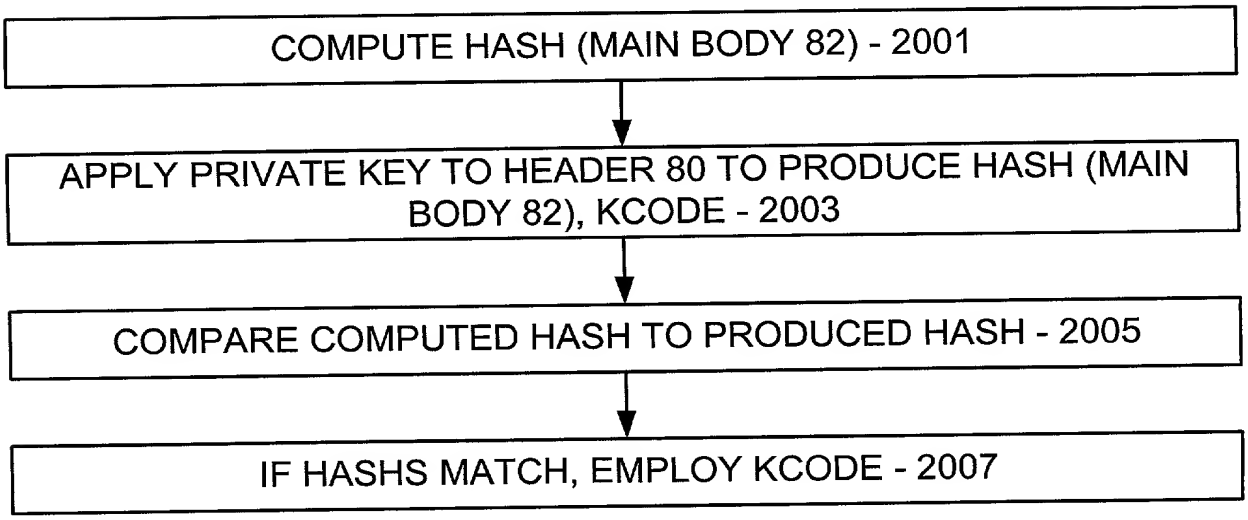

FIG. 20

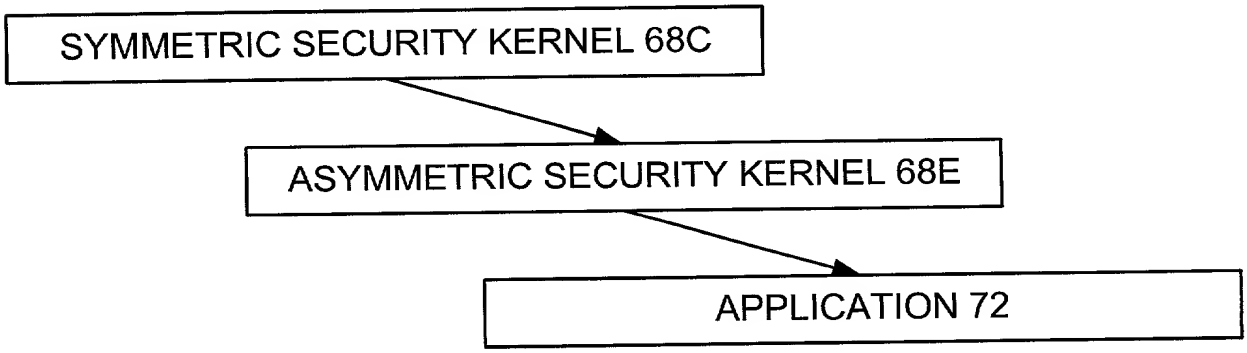

FIG. 21